

UNITED STATES DISTRICT COURT

for the
Western District of WashingtonIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Target Devices 1 & Target Devices 2, more
particularly described in attachment A-1 and
attachment A-2 respectively

Case No. MJ23-24

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Target Devices 1 from the residence at 12440 Des Moines Memorial Drive S, Burien, WA 98068, more particularly described in attachment A-1 and Target Devices 2 from the residence at 15325 1st Ave S, Burien, WA 98148, more particularly described in Attachment A-2 located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-1 and B-2, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1028A

18 U.S.C. § 1344

Aggravated Identity Theft

Bank Fraud

Offense Description

The application is based on these facts:

- ☒ See Affidavit of Eric Huynh, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Eric Huynh, Postal Inspector

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/19/2023

Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

INTRODUCTION AND AGENT BACKGROUND

2. I am a Postal Inspector (INSP) with the United States Postal Inspection Service (USPIS). I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7). I am currently assigned to the USPIS Seattle Field Division in Seattle, WA.

² Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. I became federal law enforcement officer in 2010. I have been a Special Agent in the United States Army Criminal Investigation Division, the Social Security Administration Office of the Inspector General, the Department of Homeland Security Office of the Inspector General, and the United States Postal Inspection Service, where I am currently employed. Throughout my career as a federal law enforcement officer, I have received training for and conducted many investigations related to fraud, identity theft, and bank and wire fraud. In my current assignment as a Postal Inspector, I am responsible for investigating criminal offenses related to the United States mail system, which includes theft, fraud, violence against employees, damage to postal property, and trafficking. During the course of these investigations, I have routinely applied for and carried out State and Federal search warrants, and subpoenas.

4. The facts set forth in this affidavit come from my investigative knowledge, direct participation in this investigation, information obtained from other law enforcement personnel, interviews with witnesses, and relevant documents and reports. I have not included every fact known to me or other law enforcement personnel concerning this investigation, and have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1028A (Aggravated Identity Theft), 18 U.S.C. §1344 (Bank Fraud), and 18 USC 471 (Manufacturing of Counterfeit United States Securities) will be found on the electronic devices described further below.

IDENTIFICATION OF THE SUBJECT DEVICES TO BE EXAMINED

5. The **Target Devices** include the following:

a. Electronic devices and media seized by the Washington State Department of Corrections, on April 11, 2022, from the residence at 12440 Des Moines Memorial Drive S, Burien, WA 98068 (“**Target Devices 1**”), more particularly described in attachment A-1.

B. Initial USPS Investigation

7. On November 2, 2022, INSP Kilgallen interviewed Mello. After being advised of her Constitutional rights, Mello admitted she and Hoston carried out burglaries at US Post Offices throughout Washington State in the cities of Bremerton, Port Orchard, Kirkland, Bellevue, and Tukwila. Mello stated she, Hoston, and other partially identified associates, drove their vehicle to the loading dock of a targeted Post Office and would steal large quantities of mail being processed at the Postal facility. She also admitted to stealing mail from mailboxes. During the interview she described she was in a very abusive relation with Hoston and stated he would subject her to significant physical and psychological abuse if she did not follow his directions.

8. During INSP Kilgallen's investigation, he learned Mello and Hoston were released from WA DOC supervision in September 2022, and he made WA DOC aware Mello and Hoston were being investigated. During her interview with INSP Kilgallen,

1 Mello stated she knew WA DOC Community Corrections Officer (CCO) Anne Hudson
2 very well.

3 **C. Washington State DOC and Tyrone Fareed**

4 9. On April 11, 2022, CCO Hudson attempted to arrest Tyrone Fareed, who
5 had been on community custody since October 2020, at 12440 Des Moines Memorial Dr
6 S., Burien, WA 98068. This was the primary residence of Hoston and Mello, and Fareed
7 is Mello's son. Fareed was the subject of an arrest warrant related to community custody
8 supervision violations. He was not located, and the warrant was still outstanding at the
9 time of this affidavit.

10 10. Mello was present when CCOs came to arrest Fareed, and she allowed the
11 CCOs into her residence to conduct the search. Based on information provided by Mello
12 to the CCOs, they were able to discern what property in the residence belonged to Fareed
13 and used their statutory authority to seize and search his property. CCOs found evidence
14 of Fareed's involvement with mail theft, fraudulent check manufacturing, and fraudulent
15 ID manufacturing (Licenses, Military ID's, and Passports). CCO Ronald Sivonda
16 conducted a preliminary digital examination of Fareed's electronic devices (**Target**
17 **Devices 1**), which Fareed was not permitted to possess according to the conditions of his
18 supervision and therefore were subject to search. CCO Sindova found further evidence
19 supporting Fareed was participating in crimes related to ID Theft and Bank Fraud while
20 under community supervision. CCO Sivonda reported when he found evidence of new
21 crimes on Fareed's electronic devices, he ceased his search pending the issuance of a
22 search warrant.

23 11. During WA DOC's investigation, they learned Fareed was the subject of
24 another investigation being conducted by the Bellevue Police Department (BPD) in
25 Bellevue, WA (Case No. 22-16196), and they turned over the evidence related to Fareed
26 to BPD for further investigation (*Note: According to CCO Husdon, WA DOC is limited in*
27 *their scope to investigate additional suspected crimes believed to be committed by those*
28

1 *under DOC supervision, and any evidence of new crimes must be referred to other law*
 2 *enforcement agencies).*

3 12. On December 9, 2022, INSP Huynh contacted Detective (DET) Ashley
 4 Elliot, BPD, and she stated the victim in their investigation reported Fareed used her
 5 identity to open bank accounts so he could pass fraudulent checks, and purchase vehicles.
 6 I took custody of evidence from BDP, which included: **Target Devices 1**, mail, checks,
 7 real and fake identifying documents, bank cards from BPD, and suspected ID
 8 manufacturing materials.

9 **D. Washington State DOC and 15325 1st Ave S Burien, WA**

10 13. On November 8, 2022, CCO's searched the residence of Shaun Cuvreau,
 11 15325 1st Ave S Burien, WA after he violated the terms of his supervision when he failed
 12 a routine urinalysis. Cuvreau entered community custody on February 2021, and WA
 13 DOC, CCOs used their statutory authority to search Cuvreau's property and residence.
 14 After Cuvreau failed his urinalysis, he admitted to CCOs a search of his residence would
 15 yield fentanyl and counterfeit currency. When CCOs arrived at Cuvreau's residence, they
 16 encountered a person named Albert Fellers, who was also under WA DOC supervision.
 17 Fellers answered the door holding a container of pills that were marked "M30," which is
 18 a common marking for fentanyl pills. Based on this, Fellers was taken into custody.

19 14. The search of Cuvreau's residence by WA DOC and the King County
 20 Sheriff's Office (KCSO) found evidence Cuvreau's home was being used as a
 21 manufacturing location for fraudulent ID's and counterfeit currency. They also recovered
 22 a large volume of mail, bank cards, and check—a majority of these items were associated
 23 with people who did not live at 15325 1st Ave S Burien, WA. Some of the bank cards
 24 displayed Cuvreau's name.

25 15. While examining the evidence related to fraudulent ID's, CCO Hudson saw
 26 a photo of Michael Hoston affixed to a fake Washington State ID with a different name
 27 and information. CCO Hudson recognized Hoston because in the past she has been his
 28 assigned CCO while he was under community supervision and knew he was in a close

1 relationship with Mello. After seeing this, CCO Hudson contacted INSP Kilgallen to
2 notify him of her findings.

3 16. All evidence from the search of 15325 1st Ave S Burien, WA was retained
4 by the KCSO in SeaTac, WA.

5 **D. USPIS Continued Investigation**

6 17. On November 9, 2022, INSP Kilgallen and I went to the KCSO in SeaTac,
7 WA, to review evidence seized from 15325 1st Ave S Burien, WA. The evidence
8 consisted of credit cards, fake ID's, stolen mail, **Target Devices 2**, card printer, an
9 embossing device, and suspected counterfeit US Currency. I took custody of the evidence
10 from KCSO and entered it into evidence and storage at the USPIS Headquarters in
11 Seattle, WA.

12 18. On November 9, 2022, INSP Kilgallen and I interviewed Fellers at the
13 South Correctional Entity (SCORE), in SeaTac, WA. After being advised of his
14 Constitutional rights, Fellers admitted he was part of a group of people that routinely
15 stole mail, illegally obtained people's identifying information from the Dark Web, used
16 that information to activate stolen credit cards, created fake IDs using the computers
17 seized from 15325 1st Ave S Burien, WA, and used the fake IDs to carry out additional
18 acts of fraud and theft such as cashing checks. Fellers stated he carried out these activities
19 under the direction and guidance of Kandis Mello.

20 19. Fellers described how they carried out these activities in detail. He
21 personally observed Mello create a fake ID on his computer using someone else's
22 information to activate a credit card she stole from the mail. He then took Mello to
23 Seattle, WA where she rented a BMW SUV from the SIXT rental company—this was the
24 same BMW SUV Mello and Hoston were arrested in by the Port Gamble Police
25 Department. Fellers stated he personally participated in mail theft with Mello and Hoston
26 in the BMW and stated there were times when the BMW was “stuffed” full of mail.
27 Mello and Hoston would transport the mail they stole to their residence at 12440 Des
28 Moines Memorial Dr S., Burien, WA 98068, which was also the residence of Tyrone

1 Fareed, to sort through the mail for significant items such as checks, credit cards, and
2 documents with identifying information. Once the stolen mail was sorted, they
3 transported it to Cuvreau's residence at 15325 1st Ave S Burien, WA, where they used
4 **Target Devices 2** seized by KCSO to purchase people's information from a Dark Net
5 website called "just-kill.pro." After they obtained the information, they used it to activate
6 the stolen credit cards either online or over the phone. Fellers admitted to using the credit
7 cards for general purposes such as food and gas. Regarding Mello and Hoston's use of
8 the credit cards, Fellers related they used them to make high dollar purchases from
9 designer stores such as Gucci.

10 20. Fellers stated Mello and another person identified as "Geo" were teaching
11 him how make fake ID's and research people's information to activate credit cards. He
12 admitted to knowing the information they were using to activate the cards were
13 associated with real people. According to Fellers, he and Mello used **Target Devices 2** to
14 create the ID's and research people's information.

15 21. Fellers stated at the time of his arrest on November 9, 2022, by the KCSO,
16 he was at 15325 1st Ave S Burien, WA to dispose of evidence because he was aware
17 Cuvreau was under WA DOC supervision and would fail is scheduled urinalysis, which
18 meant Cuvreau's residence at 15325 1st Ave S Burien, WA, would be searched. This is
19 further corroborated by CCO Hudson, who stated to me when they arrived at 15325 1st
20 Ave S Burien, WA, much of the evidence was organized in bags and appeared to be
21 ready for transport.

22 22. On November 9, 2022, INSP Kilgallen and I interviewed Shaun Cuvreau at
23 SCORE. After being advised of his Constitutional rights, Cuvreau admitted his residence,
24 15325 1st Ave S Burien, WA, was being used "base of operations" for identity theft
25 and bank fraud schemes. He stated Mello, Hoston, and another person named Brian
26 Tiedeman, would bring credit cards and checks they stole from the mail to his
27 residence. Once at the residence, they activated the cards so they could use them.
28

1 He explained, they obtained peoples' information from the internet and provided
2 that information to Cuvreau so he could call and activate the cards. He was aware
3 the information he used to activate the cards belonged to real people. He stated
4 after the cards were activated, he kept some and used them for gas and cigarettes.
5 Cuvreau was also aware his residence was being used to manufacture counterfeit
6 US currency.

7
8 23. Cuvreau admitted he was approached by Mello and Hoston for the
9 specific reason of using his residence for criminal activity, and he gave them his
10 consent. It was Cuvreau's belief the operation was going to be smaller in scale,
11 however it continued to expand. According to Cuvreau, Kandis would pay him for
12 the use of his residence with stolen credit cards and drugs. Cuvreau related at one
13 point he asked Mello to stop using his residence for their criminal activity, but
14 Mello threatened Cuvreau by stating she would turn him in if she were ever caught.

15 24. Curveau admitted to assisting Mello and Hoston with burglaries at US
16 Post Offices. His role in the burglaries was to conduct reconnaissance on the
17 loading docks of a targeted Post Office to see if there were any mail containers on
18 the docks and report back to Mello. Cuvreau related he didn't like participating in
19 these activities, and on a few occasions reported false information to Mello that
20 were wasn't any mail on the loading docks.

21 25. On November 10, 2022, I reviewed the evidence obtained by KSCO
22 in more detail. There was a large volume of mail that was not addressed to 15325
23 1st Ave S Burien, WA, numerous credit cards not issued to residents of 15325 1st Ave S
24 Burien, WA, and suspected counterfeit US currency.

25
26 26. Further examination of the US currency with INSP Michael Fischlin (a
27 former US Secret Service Agent), confirmed the currency was counterfeit. This was
28 based on attempts at replicating water marks, security bands with microprinting, and

1 color shifting ink. The watermarks bled through the back of the bills, the microprinting
 2 was illegible, and the locations for the color shifting ink stayed uniform while observing
 3 it from different angles.

4 **E. Investigative Conclusions**

5 27. Based on the previously stated facts and information I believe Kandis
 6 Mello, Michael Hoston, Tyrone Fareed, Albert Fellers, Shaun Cuvreau, and other known
 7 and unknown associates cooperated in an organized manner to steal mail from US Post
 8 Offices and members of the public and used the mail to further schemes related to ID
 9 Theft and Bank Fraud, and to manufacture counterfeit US currency. The primary tools
 10 they used to further these schemes were **Target Devices 1 and Target Devices 2** seized
 11 by WA DOC and KSCO, which are now in USPIS possession.

12 **Target Devices 1 and Target Devices 2** are currently in storage at **USPIS Seattle**
 13 **Division Headquarters evidence room, located at 301 Union, Seattle, WA.** In my
 14 training and experience, I know that **Target Devices 1 and Target Devices 2** have been
 15 stored in a manner in which their contents are, to the extent material to this investigation,
 16 in substantially the same state as they were when **Target Devices 1 and Target Devices**
 17 **2** first came into the possession of USPIS.

18 **TECHNICAL TERMS**

19 28. Based on my training and experience, I use the following technical terms to
 20 convey the following meanings:

21 a. Wireless telephone: A wireless telephone (or mobile telephone, or
 22 cellular telephone) is a handheld wireless device used for voice and data communication
 23 through radio signals. These telephones send signals through networks of
 24 transmitter/receivers, enabling communication with other wireless telephones or
 25 traditional "land line" telephones. A wireless telephone usually contains a "call log,"
 26 which records the telephone number, date, and time of calls made to and from the phone.
 27 In addition to enabling voice communications, wireless telephones offer a broad range of
 28 capabilities. These capabilities include: storing names and phone numbers in electronic
 "address books;" sending, receiving, and storing text messages and e-mail; taking,
 sending, receiving, and storing still photographs and moving video; storing and playing
 back audio files; storing dates, appointments, and other information on personal

1 calendars; and accessing and downloading information from the Internet. Wireless
2 telephones may also include global positioning system (“GPS”) technology for
3 determining the location of the device.

4 b. IP Address: An Internet Protocol address (or simply “IP address”) is
5 a unique numeric address used by computers on the Internet. An IP address is a series of
6 four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every
7 device attached to the Internet must be assigned an IP address so that Internet traffic sent
8 from and directed to that device may be directed properly from its source to its
9 destination. Most Internet service providers control a range of IP addresses.

10 c. Internet: The Internet is a global network of computers and other
11 electronic devices that communicate with each other. Due to the structure of the Internet,
12 connections between devices on the Internet often cross state and international borders,
13 even when the devices communicating with each other are in the same state.

14 29. Based on my training and experience, information obtained during this
15 investigation, and my discussions with other officers and agents, I know the following:

16 30. Identity (ID) theft and financial crimes are often committed in conjunction
17 with one another. Those who commit these offenses create fake IDs or utilize identifying
18 information belonging to other people to create new bank accounts or take over existing
19 accounts, and deposit illegally obtained funds or steal funds from actual account holders.

20 31. Modern ID theft and bank fraud schemes are generally initiated through the
21 internet by using digital devices such as: laptop computers, personal computers, or
22 smartphones. The reason for this is because the information required to carry out these
23 schemes is readily available through the internet, which is accessed using the
24 aforementioned types of devices. The anonymity provided by the internet makes it
25 possible for people who want to commit ID theft and bank fraud to fully assume their
26 targets’ identities, allowing them to open or take over bank accounts. Whoever has the
27 information can also call financial institutions and pose as their current target. Using the
28 information obtained from the internet, they can answer identity verification questions
that authorize banks to provide and change information on the caller’s request. The
information that can be changed—either by phone or through the internet—includes

1 mailing addresses, phone numbers, payment information, and account passwords. It can
2 also be used to order checks or have new bank cards issued under the stolen identity.

3 32. Another version of ID theft and Bank fraud schemes originates from the
4 mail. A person who steals mail can intercept bank cards and checks sent by financial
5 institutions to customers through the United States Postal Service (USPS). The person(s)
6 in possession of the stolen mail can acquire identifying information that directly targets
7 the actual customer and use their information to activate the bank card or create
8 fraudulent identification to cash stolen checks.

9 33. The information used to carry out ID theft and financial crimes can be
10 obtained via the internet through subscription-based data websites, or through websites
11 that are categorized as “Dark Web.” The subscription-based websites offer users the
12 ability to purchase personal information such as driver’s license numbers, social security
13 numbers (SSNs), and address information. Some examples of these websites include, but
14 are not limited to, Spokeo, TruthFinder, and Clear. The term “Dark Web” refers to
15 websites that allow users to purchase illegal items or information.

16 34. Possession of another person’s identifying and financial information
17 enables one to create fraudulent identification documents with real information. For
18 example, someone who obtained a state driver’s license number would be able to
19 manufacture a fake license with a verifiable identification number on it. To manufacture a
20 fake driver’s license, the appropriate equipment would be required, such as a camera,
21 computer, card printer, and laminator. The fraudulent banking information and the fake
22 IDs can be used to open lines of credit, pass forged and fraudulent checks, and make
23 online purchases.

24 35. Another crime associated with this investigation is the counterfeiting of US
25 currency. In these cases, many of the same tools used to create fraudulent ID’s can be
26 used to create counterfeit money—such as computers and printers. To create viable
27 counterfeit money, counterfeiters often attempt to replicate security features imbedded in
28 real US currency. These features may include watermarks, color shifting ink, and security

1 ribbons. These features are very difficult to replicate without specialized equipment, and
 2 most attempts to manufacture counterfeit currency are made using standard printers
 3 available to public, which results in replicated security features that are poorly presented
 4 on counterfeit currency.

5 36. During past investigations, I have personally observed that people who
 6 commit ID theft and bank fraud maintain the information in an organized manner. They
 7 do this because: the information costs them money to obtain, it makes it easier for them
 8 to reference when trying to open accounts, and keeping the information allows them to
 9 use it multiple times. I have also learned that someone who manufactures and uses
 10 counterfeit currency will keep digital images of currency so they can readily produce
 11 more when needed. Across all these crimes, evidence can present in the form of a paper
 12 notebooks and documents or electronic files on computers and electronic media.

13 **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

14 37. As described above and in Attachments B-1 and B-2, this application seeks
 15 permission to search for evidence, fruits and/or instrumentalities that might be found on
 16 **Target Devices 1 and Target Devices 2**, in whatever form they are found. One form in
 17 which the evidence, fruits, and/or instrumentalities might be found is data stored on
 18 digital devices³ such as computer hard drives or other electronic storage media.⁴ Thus,
 19 the warrant applied for would authorize the search of digital devices or other electronic
 20

21
 22 ³ “Digital device” includes any device capable of processing and/or storing data in electronic form,
 23 including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers,
 24 computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters,
 25 monitors, and drives intended for removable media, related communications devices such as modems,
 26 routers and switches, and electronic/digital security devices, wireless communication devices such as
 mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”),
 iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices
 (GPS), or portable media players.

27 ⁴ Electronic storage media is any physical object upon which electronically stored information can be
 28 recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other
 magnetic or optical media.

1 storage media or, potentially, the copying of electronically stored information from
2 digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

3 38. *Probable cause.* Based upon my review of the evidence gathered in this
4 investigation, my review of data and records, information received from other agents and
5 investigators, and my training and experience, I submit there is probable cause to believe
6 that evidence, fruits, and/or instrumentalities of the crimes of 18 U.S.C. § 1028A
7 (Aggravated Identity Theft), 18 U.S.C. § 1344 (Bank Fraud), and/or 18 USC 471
8 (Counterfeiting) will be stored on **Target Devices 1 and Target Devices 2**. I believe
9 digital devices or other electronic storage media are being or have been used to: (i) search
10 for identifying information belonging to other people on the internet; (ii) create electronic
11 records associated with the identifying information (such as lists, spreadsheets, or
12 account applications); (iii) access banking websites for the purpose of creating and using
13 fraudulent bank accounts; (iv) create fraudulent identification cards; and (v) create and
14 print counterfeit US currency. I expect that digital devices will contain critical evidence
15 of these crimes, to include: (i) communications with and/or payments to database website
16 and/or Dark Web providers; (ii) documents containing identifying information that does
17 not belong to **Mello, Hoston, Fareed, Fellers or Cuvreau**; (iii) lists of current and prior
18 identity theft victims; (iv) digital templates for manufacturing fake identification
19 documents, (v) records of communications (including phone calls) with financial
20 institutions, and (vi) templates and/images for creating and printing counterfeit US
21 currency. There is, therefore, probable cause to believe that evidence, fruits, and/or
22 instrumentalities of the crimes of 18 U.S.C. § 1028A (Aggravated Identity Theft), 18
23 U.S.C. § 1344 (Bank Fraud), or 18 USC 471 (Counterfeiting) exists and will be found on
24 **Target Devices 1 and Target Devices 2** for at least the following reasons:

- 25 a. Based on my knowledge, training, and experience, I know that computer
26 files or remnants of such files can be preserved (and consequently also then
27 recovered) for months or even years after they have been downloaded onto
28 a storage medium, deleted, or accessed or viewed via the Internet.
Electronic files downloaded to a digital device or other electronic storage

medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

39. Based on previous investigations conducted by other law enforcement agencies, and witnesses with firsthand knowledge concerning the use of **Target Devices 1 and Target Devices 2** to search for identifying information using the internet, there is reason to believe these devices were used primarily to carry out acts related to ID Theft, Bank Fraud, and counterfeiting. **Target Devices 1** were seized by WA DOC because FAREED was not allowed to be in possession of electronic devices, per his community custody agreement. **Target Devices 1** were given a preliminary examination which found templates for fake ID’s and checks. The WA DOC examiner stopped their search upon discovering the new evidence. Regarding **Target Devices 2**, these items were seized during a lawful search of **Cuvreau’s** residence at 15325 1st Ave S Burien, WA, which led

1 to the arrest of **Fellers**. During the interviews of **Fellers** and **Cuvreau**, they both stated
2 the computers were used to create fake ID's, activate stolen credit cards, and research
3 identity theft victims' information.

4 40. *Forensic evidence.* As further described in Attachments B1 and B-2, this
5 application seeks permission to locate not only computer files that might serve as direct
6 evidence of the crimes described on the warrant, but also for forensic electronic evidence
7 that establishes how digital devices or other electronic storage media were used, the
8 purpose of their use, who used them, and when. There is probable cause to believe that
9 this forensic electronic evidence will be on **Target Devices 1 and Target Devices 2**
10 because:

11 a. Stored data can provide evidence of a file that was once on the digital
12 device or other electronic storage media but has since been deleted or edited, or
13 of a deleted portion of a file (such as a paragraph that has been deleted from a
14 word processing file). Virtual memory paging systems can leave traces of
15 information on the digital device or other electronic storage media that show
16 what tasks and processes were recently active. Web browsers, e-mail
17 programs, and chat programs store configuration information that can reveal
18 information such as online nicknames and passwords. Operating systems can
19 record additional information, such as the history of connections to other
20 computers, the attachment of peripherals, the attachment of USB flash storage
21 devices or other external storage media, and the times the digital device or
22 other electronic storage media was in use. Computer file systems can record
23 information about the dates files that were created and the sequence in which
24 they were created.

25 b. As explained herein, information stored within a computer and other
26 electronic storage media may provide crucial evidence of the "who, what, why,
27 when, where, and how" of the criminal conduct under investigation, thus
28 enabling the United States to establish and prove each element or alternatively,
to exclude the innocent from further suspicion. In my training and experience,
information stored within a computer or storage media (e.g., registry
information, communications, images and movies, transactional information,
records of session times and durations, internet history, and anti-virus,
spyware, and malware detection programs) can indicate who has used or
controlled the computer or storage media. This "user attribution" evidence is
analogous to the search for "indicia of occupancy" while executing a search

warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.⁵ Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

⁵ For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

41. *Manner of Execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

42. Digital devices must have been used as instrumentalities of the crimes under investigation based on the established methods used to search for identifying information belonging to others and, for instance, to apply for bank accounts. For example, Fellers and Cuvreau admitted to participating with Mello and Hoston, and directly observing them use digital devices to search for fraudulent information on the internet, which was used to activate credit cards stolen from the mail. The information obtained could help establish key aspects of this case, including: (i) the manner and methods by which they compiled fraudulent information; (ii) that their actions in furtherance of the Aggravated Identity Theft and Bank Fraud offenses were deliberate; and (iii) that they had knowledge (through, for example, electronic searches or purchases

from online databases) that the identifying and financial information obtained belonged to other real persons.

SEARCH TECHNIQUES

43. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachments B-1 and B-2 to this Affidavit, and will specifically authorize review of the media or information consistent with the warrant.

44. Consistent with the above, I hereby request the Court's permission to obtain forensic images of **Target Devices 1 and Target Devices 2**, using the following procedures:

E. Processing the Search Sites and Securing the Data.

a. **Target Devices 1 and Target Devices 2**, which were seized by WA DOC and KCSO subsequent to a search warrant, will be sent to law enforcement personnel with appropriate expertise.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachments B-1 and B-2 to this Affidavit.⁶

⁶ The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1 c. A forensic image may be created of either a physical drive or a logical
2 drive. A physical drive is the actual physical hard drive that may be found in a
3 typical computer. When law enforcement creates a forensic image of a
4 physical drive, the image will contain every bit and byte on the physical drive.
5 A logical drive, also known as a partition, is a dedicated area on a physical
6 drive that may have a drive letter assigned (for example the c: and d: drives on
7 a computer that actually contains only one physical hard drive). Therefore,
8 creating an image of a logical drive does not include every bit and byte on the
9 physical drive. Law enforcement will only create an image of physical or
10 logical drives physically present on or within the subject device.


11 **F. Searching the Forensic Images.**

12 a. Searching the forensic images for the items described in Attachments B-1
13 and B-2, may require a range of data analysis techniques. In some cases, it is
14 possible for agents and analysts to conduct carefully targeted searches that can
15 locate evidence without requiring a time-consuming manual search through
16 unrelated materials that may be commingled with criminal evidence. In other
17 cases, however, such techniques may not yield the evidence described in the
18 warrant, and law enforcement may need to conduct more extensive searches to
19 locate evidence that falls within the scope of the warrant. The search
20 techniques that will be used will be only those methodologies, techniques and
21 protocols as may reasonably be expected to find, identify, segregate and/or
22 duplicate the items authorized to be seized pursuant to Attachments B-1 and B-
23 2 to this affidavit. Those techniques, however, may necessarily expose many
24 or all parts of a hard drive to human inspection in order to determine whether it
25 contains evidence described by the warrant.
26
27
28

CONCLUSION

45. Based on the foregoing and on my training, experience, and the investigation to date, I have probable cause to believe, and do believe, Kandis Mello, Michael Hoston, Albert Fellers, and Shaun Cuvreau, have committed offenses in violation of 18 U.S.C. § 1028A (Aggravated Identity Theft), 18 U.S.C. § 1344 (Bank Fraud), and 18 USC 471 (Counterfeiting of US Currency) and that evidence of these offenses, as more fully described in Attachments B-1 and B-2, are presently contained at the USPIS Headquarters in Seattle, WA, in the **Targets Devices 1 and Target Devices 2**, in the Western District of Washington, as more fully described above and in Attachments A-1 and A-2. I therefore request that the Court issue a warrant authorizing the government to search **Targets Devices 1 and Target Devices 2**, as described in Attachments A-1 and A-2, and to seize all the items specified in Attachments B-1 and B-2.

I declare and affirm under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.



ERIC H. HUYNH
Postal Inspector
United States Postal Inspection Service

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit by telephone on this 19th day of January, 2023.



HON. S. KATE VAUGHAN
United States Magistrate Judge

ATTACHMENT A-1**Property to Be Searched**

The property to be searched includes the following digital devices seized by the Washington State Department of Corrections on April 11, 2022 from 12440 Des Moines Memorial Dr S., Burien, WA (hereinafter the “**Target Devices 1**”).

Target Devices 1 consists of the following items:

One orange thumb drive, no serial number, depicted below:



One “Celero 5G” cellular smartphone, serial number unknown, depicted below:



One “Motorola” cellular smartphone, serial number unknown, depicted below:



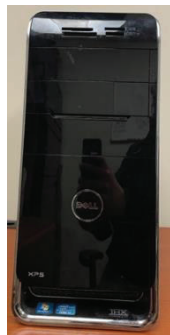
One "HGST" hard drive, serial number E182115, depicted below:



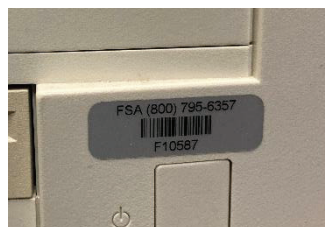
One Apple desktop computer, serial number unknown, depicted below:



One Dell XPS computer tower, serial number C33RHS1, depicted below:



One QES computer tower, serial number F10587, depicted below:





One “WD” 500 GB hard drive, serial number WMAYP0F40A41, depicted below:



One HP Laptop, serial number CND3451G2F, depicted below:

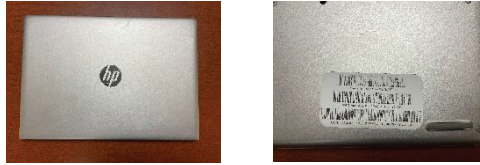


ATTACHMENT A-2**Property to Be Searched**

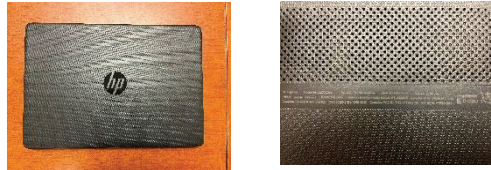
The property to be searched are digital devices seized by the King County Sheriff's department on November 8, 2022, from 15325 1st Ave S Burien, WA (hereinafter the "**Target Devices 2**").

Target Devices 2 consists of the following items:

One HP laptop, serial number 2TK9480406, depicted below:



One HP laptop, serial number 5CD219CGFV, depicted below



One Dell laptop, serial number 4C7ZWN1, depicted below:



Two thumb drives depicted below:



One Google Pixel smartphone, serial number Unknown, depicted below:



One "Moxie" cellular smartphone, serial number unknown, depicted below:



ATTACHMENT B-1**Particular Things to be Seized**

1. All records on the digital devices belonging to Tyrone Fareed, seized by the Washington State Department of Corrections on April 11, 2022 from 12440 Des Moines Memorial Dr. S., Burien, WA (hereinafter the “**Target Devices 1**”) that contain evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1028A (Aggravated Identity Theft), 18 U.S.C. § 1344 (Bank Fraud), and 18 USC 471 (Counterfeiting of US Currency) those violations involving Tyrone Fareed, and occurring between approximately October 8, 2020 to April 8, 2022:

a. Financial records, including bank statements, canceled checks, deposit records, check stubs, checkbook registers, deposit slips, loans, documentation of assets and liabilities, general ledgers, general journals, cash, cash receipts, billing information, records of transfers, and records of bills relating to the receipt of currency or other forms of payment.

b. Documents used for identification, such as state identification cards, state driver’s licenses, passports, tribal identification cards, and other forms of identifying documents.

c. Records of credit card and automatic teller machine activity, including physical credit and/or debit cards, and automatic teller machine records.

d. Notes payable and receivable, IOUs, and other recordation of debts comprising evidence of loans and expenses.

e. Papers, records, documents, files, notes, memos, mail, or other materials representing residency, ownership, occupancy, dominion, or control of the premises referenced above and described in Attachment A-1.

1 f. Records or keys showing possession of safe deposit boxes, safes,
2 storage units, and any other type of storage areas, including passwords and/or access
3 codes for access during the searches.

4 g. All contact information and correspondence to and from banks and
5 other financial institutions.

6 h. Any information regarding efforts to evade law enforcement, bank
7 or regulatory detection, civil penalties, and any information showing the receipt of legal
8 process.

9 i. Any records that contain personal identifying information that is not
10 assigned to the legal resident at 12440 Des Moines Memorial Dr. S., Burien, WA.

11 2. Evidence of user attribution showing who used or owned the **Target**
12 **Devices 1** at the time the things described in this warrant were created, edited, or deleted,
13 such as logs, phonebooks, saved usernames and passwords, documents, and browsing
14 history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs,
15 and correspondence.

16 a. Evidence of software that would allow others to control the devices,
17 such as viruses, Trojan horses, and other forms of malicious software, as well as evidence
18 of the presence or absence of security software designed to detect malicious software.

19 b. Evidence of the lack of such malicious software.

20 c. Evidence indicating how and when the **Target Devices 1** were
21 accessed or used to determine the chronological context of computer access, use, and
22 events relating to the crimes under investigation and to the **Target Devices 1** user.

23 d. Evidence indicating the **Target Devices 1** user’s state of mind as it
24 relates to the crimes under investigation.

25 e. Evidence of the attachment to the **Target Devices 1** of other storage
26 devices or similar containers for electronic evidence.

1 f. Evidence of counter-forensic programs (and associated data) that are
2 designed to eliminate data from the **Target Devices 1**.

3 g. Evidence of the times the **Target Devices 1** was used.

4 h. Passwords, encryption keys, and other access devices that may be
5 necessary to access the **Target Devices 1**.

6 3. Records of or information about Internet Protocol addresses used by the
7 **Target Devices 1**.

8 a. Records of or information about the **Target Devices 1** Internet
9 activity that may be related to the crimes alleged, including firewall logs, caches, browser
10 history and cookies, “bookmarked” or “favorite” web pages, search terms that the user
11 entered into any Internet search engine, and records of user-typed web addresses.

12 b. Contextual information necessary to understand the evidence
13 described in this attachment.

14
15 As used above, the terms “records” and “information” include all of the foregoing
16 items of evidence in whatever form and by whatever means they may have been created
17 or stored, including any form of computer or electronic storage (such as flash memory or
18 other media that can store data) and any photographic form.

ATTACHMENT B-2**Particular Things to be Seized**

1. All records on the digital devices seized by the King County Sheriff's department on November 8, 2022, from 15325 1st Ave S Burien, WA (hereinafter the "Target Devices 2") that contain evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1028A (Aggravated Identity Theft), 18 U.S.C. § 1344 (Bank Fraud), and 18 USC § 471 (Counterfeiting of US Currency), those violations involving Kandis Mello, Michael Hoston, Shaun Cuvreau, Albert Fellers, and other unknown associates, occurring between approximately February 8, 2021 to November 8, 2022:

a. Financial records, including bank statements, canceled checks, deposit records, check stubs, checkbook registers, deposit slips, loans, documentation of assets and liabilities, general ledgers, general journals, cash, cash receipts, billing information, records of transfers, and records of bills relating to the receipt of currency or other forms of payment.

b. Documents used for identification, such as state identification cards, state driver's licenses, passports, tribal identification cards, and other forms of identifying documents.

c. Records of credit card and automatic teller machine activity, including physical credit and/or debit cards, and automatic teller machine records.

d. Notes payable and receivable, IOUs, and other recordation of debts comprising evidence of loans and expenses.

e. Papers, records, documents, files, notes, memos, mail, or other materials representing ownership, dominion, or control of the vehicle referenced above and described in Attachment A-2.

1 f. Records or keys showing possession of safe deposit boxes, safes,
2 storage units, and any other type of storage areas, including passwords and/or access
3 codes for access during the searches.

4 g. All contact information and correspondence to and from banks and
5 other financial institutions.

6 h. Any information regarding efforts to evade law enforcement, bank,
7 or regulatory detection, civil penalties, and any information showing the receipt of legal
8 process.

9 i. Any records that contain personal identifying information that is not
10 assigned to the legal resident of 15325 1st Ave S. Burien, WA.

11 2. Evidence of user attribution showing who used, owned, or controlled the
12 **Target Devices 2** at the time the things described in this warrant were created, edited, or
13 deleted, such as logs, registry entries, configuration files, saved usernames and
14 passwords, documents, browsing history, user profiles, email, email contacts, “chat,”
15 instant messaging logs, photographs, and correspondence.

16 a. Evidence of software that would allow others to control the **Target**
17 **Devices 2**, such as viruses, Trojan horses, and other forms of malicious software, as well
18 as evidence of the presence or absence of security software designed to detect malicious
19 software.

20 b. Evidence of the lack of such malicious software.

21 c. Evidence indicating how and when the **Target Devices 2** was
22 accessed or used to determine the chronological context of computer access, use, and
23 events relating to the crimes under investigation and to the **Target Devices 2** user.

24 d. Evidence indicating the **Target Devices 2** user’s state of mind as it
25 relates to the crimes under investigation.

26 e. Evidence of the attachment to the **Target Devices 2** of other storage
27 devices or similar containers for electronic evidence.

1 f. Evidence of counter-forensic programs (and associated data) that are
2 designed to eliminate data from the **Target Devices 2**.

3 g. Evidence of the times the **Target Devices 2** was used.

4 h. Passwords, encryption keys, and other access devices that may be
5 necessary to access the **Target Devices 2**.

6 3. Records of or information about Internet Protocol addresses used by the
7 **Target Devices 2**.

8 a. Records of or information about the **Target Devices 2** Internet
9 activity that may be related to the crimes alleged, including firewall logs, caches, browser
10 history and cookies, “bookmarked” or “favorite” web pages, search terms that the user
11 entered into any Internet search engine, and records of user-typed web addresses.

12 b. Contextual information necessary to understand the evidence
13 described in this attachment.

14
15 As used in this attachment, the terms “records” and “information” include all of
16 the foregoing items of evidence in whatever form and by whatever means they may have
17 been created or stored, including any form of computer or electronic storage (such as
18 flash memory or other media that can store data) and any photographic form.